AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
See Attachment A to Affidavit

Case No. 3:18SW219

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*
See Attachment A, fully incorporated by reference herein;

located in the Eastern District of Virginia, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, fully incorporated by reference herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 1341,1344,1028A	Mail Fraud, Bank Fraud, Aggravated Identity Theft

The application is based on these facts:

See attached Affidavit, fully incorporated by reference herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Michael S. Bowser, FBI Task Force Officer
Printed name and title

Sworn to before me and signed in my presence.

Date: September 25, 2018

/s/
David J. Novak
United States Magistrate Judge
Judge's signature

City and state: Richmond, Virginia

David J. Novak, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF:

Toshiba laptop (S/N 3F128753C) silver in color containing two pieces of paper inside.

Hewlett Packard Laptop (Model number T9449AV, S/N SCD6248JW2) silver in color with wireless Microsoft Bluetooth connector in side slot.

Seagate External Expansion Hard Drive (S/N 2GHPCN95) black in color.

Case No. 3:18SW219

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Michael S. Bowser, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Detective with the Chesterfield County Police Criminal Investigations, Economic Crime Unit, and have been employed since September 2001. I am currently assigned as a Task Force Officer (TFO) to the Secret Service, Richmond Division and have been since

October 25th, 2017. I have participated in investigations involving financial crimes to include embezzlement, credit card theft, credit card fraud, and identity theft. I have also discussed and reviewed these materials with other law enforcement officers.

3. In the course of my employment as a sworn law enforcement officer, I have participated in the execution of numerous search warrants resulting in the seizure of computers, magnetic storage media for computers, other electronic media, and other items evidencing violations of state and federal laws, including various sections of 18 U.S.C. §§ 1344 (Bank Fraud), 1341 (Mail Fraud), and 1028A (Aggravated Identity Theft).

4. I have been deputized as a Special Deputy United States Marshal since October 25th, 2017. As a Special Deputy United States Marshal, your Affiant is authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

The property to be searched (referred to collectively as "the devices") consists of:

Toshiba laptop (S/N 3F128753C), silver in color containing two pieces of paper inside.

Hewlett Packard Laptop (Model number T9449AV, S/N SCD6248JW2)
silver in color with wireless Microsoft Bluetooth connector in side slot.

Seagate External Expansion Hard Drive (S/N 2GHPCN95) black in color.

6. The Devices are currently located at the Evidence Control Center at the main office of the Richmond Division of the Secret Service 500 Arboretum Parkway Suite 500, North Chesterfield, VA 23235.

7. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

DEFINITIONS

8. The **Internet** is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

9. **Internet Protocol address (or simply "IP address")** is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (*e.g.*, 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

10. **Storage medium** is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

11. **Log Files** are records automatically produced by computer programs to document

electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

PROBABLE CAUSE

12. On August 8th, 2018, Special Agent Doucette of the Secret Service and TFO Bowser met with Cynthia Hyatt to interview her about her husband, Daniel Hyatt. Cynthia stated Daniel Hyatt obtained credit using her information without her permission. Cynthia stated in March of 2018, she checked her credit report and found several accounts were opened that she did not open herself. Cynthia Hyatt provided Agent Doucette and TFO Bowser a copy of her credit report showing the accounts she said she did not open. Among the accounts opened without her permission was an account with American Express, a financial institution insured by the Federal Deposit Insurance Corporation. When Cynthia confronted Daniel about this, he admitted to opening accounts without her permission and typed up letters on his computer and to sending the letters to the financial institutions with the exception of the letter to American Express. A copy of one of the letters (to American Express) was provided to Agent Doucette and TFO Bowser by Cynthia Hyatt.

13. Cynthia also stated that she found money had been taken out of her children's savings accounts at Virginia Credit Union and transferred to another account without her

permission. TFO Bowser and Agent Doucette learned there were checks ordered online from Virginia Credit Union from Cynthia Hyatt's childrens' saving accounts. Virginia Credit Union is a financial institution with its deposits insured by the National Credit Union Administration's Share Insurance Fund. Cynthia did not order the checks and did not authorize the transactions. The checks were issued from Virginia Credit Union and sent in the mail to the address of 1713 Warminster Drive Midlothian, Virginia 23113. The checks were deposited into a Suntrust Bank account through an ATM deposit. The account the deposit was placed into was an account Cynthia did not open. After reviewing the bank statements from Suntrust, the money was moved into another Suntrust Account. That Suntrust account is another one that Cynthia did not open. The account was opened in her name using her personal information. It is believed Daniel Hyatt was the one who received the checks in the mail. Cynthia stated Daniel was working from home as a day trader and would have access to the mail while Cynthia was at work.

14. Cynthia stated Daniel convinced her to sell her residence which she owned outright and give him $50,000 from the sale for him to invest. Cynthia stated Daniel would show her statements from an E-Trade account showing the couple had an approximate balance of $900,000 in the account. Daniel also showed her emails from an A-Z Investment Club claiming the balance of the E-Trade account was now in an account managed by the club. As shown below, the E-Trade statements produced by Daniel Hyatt were fraudulent and the emails from A-Z Investments were actually created by Daniel Hyatt and were fraudulent as well.

15. Cynthia also stated she had applied for financial assistance through St. Edward the Confessor Catholic Church located at 2700 Dolfield Road, North Chesterfield, VA 23235.

Cynthia was told by the church they had provided assistance to her husband Daniel Hyatt two years prior. When Cynthia asked her what it was for, they said rent.

16. Cynthia stated Jennifer Snider from St. Edward the Confessor Catholic Church provided her a copy of the lease agreement her husband provided the church as proof of his need for rental assistance. The lease showed a Taylor Baker was the landlord, and it was for the address of 1713 Warminster Drive, Midlothian, VA 23113. The address was the address that Cynthia and Daniel were living at the time Daniel requested assistance from St. Edward the Confessor Catholic Church. Cynthia stated on the date of the lease and at the time of her husband's request for rental assistance, Cynthia's mother owned the house at 1713 Warminster Drive. The records from Chesterfield County Real Estate Assessment show Patricia Faulconer owned the house at the time the church provided rental assistance. Patricia is Cynthia's mother. St. Edward the Confessor Catholic Church mailed a check to Taylor Baker at 6189 Rim Fire Road Mechanicsville, Virginia 23111.

17. On August 14th, 2018 Agent Doucette and TFO Bowser met with Taylor Baker at his place of employment. Taylor stated he never owned the house listed in the lease of 1713 Warminster Drive Midlothian, VA 23113. Taylor stated he did not own any rental properties and did not create the lease Daniel Hyatt presented to St. Edward the Confessor Catholic Church. Taylor and Daniel were former co-workers. Taylor stated Daniel asked him to cash a check. Taylor stated he received the check from St. Edward the Confessor Catholic Church in the mail. Taylor stated he took the check, cashed it, and gave the money to Daniel Hyatt. Taylor stated he did not receive any money from cashing the check.

18. On August 13th, 2018 Agent Doucette appeared before Senior U.S. District Judge Henry E. Hudson and obtained an arrest warrant via criminal complaint charging Daniel with Mail Fraud. On August 14th, 2018, Daniel Hyatt met with his Probation Officer, Jami Pease from Federal Probation. Pease interviewed Daniel Hyatt prior to him being taken into custody by the United States Marshals.

19. Daniel Hyatt was questioned by Pease about the assistance he received from St. Edward the Confessor Catholic Church for the rent. Daniel stated he did not received any rental assistance in 2016. FPO Pease asked Daniel who Taylor was, Daniel said he was not sure.

20. Pease asked Daniel about why his wife is angry at him. Daniel said it was because of his dishonesty. Pease asked Daniel what he meant by that. Daniel said there are too many lies to recount. Pease asked Daniel about the credit cards opened up in her name. Daniel denied she did not know about the cards and they had talked about opening the cards. Daniel did state she did not know that he charged them up and it is his fault he has ruined her credit.

21. Pease asked Daniel why he wrote the letters to the credit card companies. Daniel said he wanted to help Cynthia. FPO Pease asked Daniel if he used fake E-trade statements and other falsified documentation that would lead Cynthia to believe she could spend more money freely. Daniel replied yes.

22. Pease asked Daniel about A to Z Investments. He stated it was all made up. Daniel stated he made up the investment club and he was the one emailing himself and Cynthia, portraying himself as the president of the investment club. Daniel stated there was no money hidden. All the emails were generated by Daniel Hyatt to make it look like he was communicating with someone from A to Z Investments.

23. Cynthia stated Daniel had two laptops that he kept in a back pack. He used a laptop on a regular basis for his purported day trading activities conducted from the house they shared. In or around July 31st, 2018, Cynthia had confronted Daniel about some purported employment, particularly a paycheck Daniel claimed to have received from his employer. Cynthia stated that during the ensuing discussion, Daniel told her the backpack was stolen along with the laptop computers and in their bank account. TFO Bowser conducted a search of Law Enforcement Databases for any police report filed by Daniel Hyatt with negative results.

24. On August 17th, 2018, FPO Jami Pease contacted Agent Doucette and advised Leslie Hyatt, the ex-wife of Daniel Hyatt, called about two laptops her daughter had. Leslie Hyatt stated to FPO Pease, her daughter received two laptops from Daniel Hyatt. Agent Doucette and TFO Bowser responded to 1746 Early Settlers Road, North Chesterfield, Virginia 23325. Leslie Hyatt did not want the laptops in her house and turned them over to Agent Doucette and TFO Bowser.

25. The credit accounts that Cynthia Hyatt maintains were opened in her name by Daniel Hyatt were opened on-line using a computer, and the unauthorized ordering of the checks from her childrens' bank accounts. Furthermore, the only practicable means by which Daniel could create the false emails, E-Trade statements, and false lease referenced previously is through the use of a computer. Finally, Daniel's apparently false statement to Cynthia about his computers having been stolen, when in fact, they were at his ex-wife's house, supports the inference that Hyatt knew the computers had incriminating information on them.

26. On August 22nd, 2018, TFO Bowser received a call from Cynthia Hyatt. She stated she found an external hard drive that did not belong to her or her children in the residence.

The external hard drive was found in the back of a downstairs closet. Cynthia turned over the external hard drive to TFO Bowser, and TFO Bowser turned it over to the Secret Service. Based on my training and experience, external hard drives are used to store large amounts of electronic data to include documents and other electronic files similar to those discussed previously.

27. The Devices are currently in the possession of the Secret Service Office in connection with a Secret Service investigation of allegations that Daniel Hyatt violated Title 18, United States Codes (U.S.C.), §§ 1341, 1344, and 1028A. The items to be searched for and seized under this warrant are described more particularly in Attachment B, incorporated herein by reference.

28. The Devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the Secret Service on August 17th, 2018 and August 22nd, 2018.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

29. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

30. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

31. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

33. *Manner of execution.* Because this warrant seeks only permission to examine the Devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

NOTICE REGARDING INITIATION OF FORENSIC EXAMINATION

34. Moreover, the Government will file a written pleading in this case within one hundred twenty (120) days after the execution of the search warrant notifying the court that the imaging process of digital evidence seized from the target location is complete, and the forensic analysis of computers and media has begun. Such notice will include confirmation that written notice has been provided to the defendant or his counsel informing the defendant that the forensic examination of evidence seized from him has actually begun. Such notice to the defendant and the Court is not intended to mean, and should not be construed to mean, that the forensic analysis is complete, or that a written report detailing the results of the examination to date will be filed with the Court or provided to the defendant or his counsel. This notice does not create, and is not meant to create, additional discovery rights for the defendant. Rather, the sole purpose of this notice is to notify the defendant that, beyond the simple seizure of his property, a forensic search of that property has actually begun.

CONCLUSION

35. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Michael Bowser TFO
Special Deputy United States Marshal
Secret Service Financial Crimes Task Force

SEEN AND APPROVED BY:

Michael C. Moore
Assistant United States Attorney

Subscribed and sworn to before me on September 25, 2018.

/s/
David J. Novak
United States Magistrate Judge

ATTACHMENT A

The property to be searched (referred to collectively as "the devices") consists of:

Toshiba laptop (S/N 3F128753C) silver in color containing two pieces of paper inside.

Hewlett Packard Laptop (Model number T9449AV, S/N SCD6248JW2) silver in color with wireless Microsoft Bluetooth connector in side slot.

Seagate External Expansion Hard Drive (S/N 2GHPCN95) black in color.

The devices are currently located at the Evidence Control Center at the main office of the Richmond Secret Service, 500 Arboretum Parkway Suite 500, North Chesterfield, VA 23235.

This warrant authorizes the forensic examination of the devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

The evidence to be seized is the fruits, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1341 (Mail Fraud) 1344 (Bank Fraud) and 1028A(a)(1) (Aggravated Identity Theft), including, but not limited to the following:

1. Unauthorized or fraudulent credit card, bank, or credit union account applications and communications (whether in electronic or other format) and correspondence regarding the same;
2. Fraudulent leases and correspondence (whether in electronic or other format) regarding the same;
3. Records regarding the on-line ordering of checks and transfers of monies to and from accounts at financial institutions;
4. Records regarding the on-line purchase of goods or services;
5. Internet searches to visits to websites regarding items 1-4; and

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTERS"):

    a. evidence of who used, owned, or controlled the COMPUTERS at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTERS, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTERS of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTERS;

f. evidence of the times the COMPUTERS was used;

g. records of or information about Internet Protocol addresses used by the COMPUTERS;

h. records of or information about the COMPUTERS' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

i. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.